President’s Letter

By Anna Kuperman
President
M: 0419 803 263

Dear Members

Spring is here and iappANZ is springing into Privacy@Work 2015. Our Early Bird Pricing is ending soon so to take advantage of the special Summit rates REGISTER HERE.

This month, we welcome three new sponsors to our iappANZ sponsor community. On behalf of the Board, I welcome our new:

- platinum sponsor, the National Association of Information Destruction ANZ (NAID);
- gold sponsor, Telstra; and
- silver sponsor, Minter Ellison.

Cross collaboration across industries is key to connecting privacy people and enhancing privacy practice. We are grateful for the valuable insight and connections that these organisations can bring to our association and our members. Our Summit participant list showcases leading experts working in diverse areas and disciplines yet privacy forms an important focus in their professional lives. Come along to hear from the following panelists:

- Anne Marie Allgrove, Partner, Baker & McKenzie
- Adrian Anderson, former GM, AFL Football Operations and Media, Sports Law Barrister
- Ron Bartsch, Leading Aviation Expert & Chairman, UAS International
- Russell Burnard, Government Chief Privacy Officer, Internal Affairs, New Zealand
- Ben Carr, Chief Privacy Officer, Telstra
- Paul Czarnota, Barrister, Victorian Bar, Attorney, New York State Bar
- Dr Grant Davies, Commissioner, Victorian Health Services
- Angelene Falk, Assistant Commissioner, Regulation and Strategy Branch, OAIC
- Patrick Gray, Information Security Journalist, Risky Business Podcaster and Blogger
- Gail Hambly, Group General Counsel & Company Secretary, Fairfax Media Limited
- Ros Harvey, Founder and Managing Director, The Yield
Finally, a comment from me and your feedback is encouraged. Who remembers the outrage that hit the headlines a couple of years ago when the founder of Facebook, Mark Zuckerberg, declared that privacy was dead in the age of digital social media?

With the new metadata retention laws coming into effect from 13 October 2015, the same theme is triggering raw nerves in the press and community. What’s your view? Are we keeping privacy on life support in the digital age? Can we redefine privacy in the digital age – away from keeping things under lock and key but with different guide posts of trust, transparency and accountability?

Our editors would be thrilled to publish member feedback in our next journal. Please email to our editors: Veronica Scott (veronica.scott@minterellison.com) and Carolyn Lidgerwood (carolyn.lidgerwood@riotinto.com)

Happy reading!

Anna
Dear Members

Welcome to the September issue of Privacy Unbound. This month’s edition contains celebrity gossip, sex, lies and videotape. Not to mention strategic privacy assessments, data breach notification and ethics in human research.

We kick off with the critical question of whether Bradley Cooper is a bad tipper. Anna Johnston, privacy expert extraordinaire and Director of Salinger Privacy looks at how the publication of the NYC taxi dataset illustrates a particular challenge for privacy professionals: how easily an individual’s identity, pattern of behaviour, physical movements and other traits can be extrapolated from a supposedly ‘anonymous’ set of data, published with good intentions in the name of ‘open data’, public transparency or research.

Does David Watts, Victoria’s inaugural Commissioner for Privacy and Data Protection favour mandatory data breach notification? How does he rate Australia and Victoria in particular in relation to privacy rights and protections? What books is David reading at the moment? Find out more in this Q&A with Veronica Scott, Special Counsel at Minter Ellison Lawyers, iappANZ board member and co-editor of Privacy Unbound.

Big data and privacy in human research – a legal or an ethical problem or both? What privacy questions should researchers and ethics committees be asking when research involves digital data, including data linkage? Jodie Mcvernon, Deborah Warr and Assunta Hunter from the University of Melbourne write about their engagement with a broad cross-disciplinary and cross-sectoral group to develop a consultation document entitled ‘Guidelines for the Ethical Use of Digital Data in Human Research’.

Next up is our regular column with the Acting Australian Information Commissioner, Timothy Pilgrim. This month Timothy sheds some light on the current status of the OAIC and how he sees the Office operating through the mid to longer term. He also highlights the role of strategic privacy assessments in identifying specific or potential problems with information gathering, handling or management and the sectors that are the immediate focus of assessment for the OAIC. How should organisations treat metadata whilst his determination in Ben Grubb v Telstra Corporation Limited awaits appeal before the AAT? For all this and more, turn to page 11.

From sex, lies and video tapes to class actions. Emma Hossack, CEO of Extensia and Binder, Vice-President of the Medical Software Industry Association, and iappANZ Board director exposes the hidden world of privacy litigation, drawing on presentations by Michael Rivette, a Melbourne-based barrister who specialises in privacy litigation. You can hear more directly from Michael at the iappANZ Privacy@Work Summit in Melbourne on 18 November 2015.

Whilst we all eagerly await news about the introduction of mandatory data breach notification laws in Australia, Carolyn Lidgerwood, Global Privacy Counsel at Rio Tinto, iappANZ board member and co-editor of Privacy Unbound takes us to Canada and the European Union, for comparison with developments in Australia and New Zealand as they unfold.

Will any of these authors be the winner of this year’s writing prize? If you’d like to know (and perhaps judge them for yourself), turn to page 20 for the rules!

Finally, there are only 7 weeks until the iappANZ Privacy@Work Summit. Join us in Melbourne to hear from the world’s leading privacy experts and mingle with Australia’s finest. To take advantage of our special Early Bird Rate before 7 October 2015, REGISTER HERE.

We hope you enjoy this edition of Privacy Unbound.

Melanie

Vice-President’s Foreword

By Melanie Marks

Vice-President

melanie.marks@cba.com.au
A message about iappANZ membership:

Membership benefits

iappANZ has grown into the pre-eminent forum for people with an interest in privacy in Australian and New Zealand, offering our members a wealth of opportunities to expand their privacy knowledge, compliance, interests and networks. We continue to work with private entities across all industry sectors as well as regulators in both countries.

As an iappANZ member you are entitled to receive a range of great member benefits as outlined at: www.iappanz.org.

Through our affiliation with the global body, the International Association of Privacy Professionals (iapp), you are also entitled to additional member benefits, including the knowledge and resources located within the members' only area of the iapp website at: www.privacyassociation.org.

You can access benefits available to you through your iapp account. Simply login to your MyIAPP account using your email address as the username. If you do not yet have a password or have forgotten yours just click on the “Reset your password” link and instructions on how to create a new password will be sent to you. If you don't want us to confirm your membership details to iapp in accordance with iappANZ's privacy policy, please let me know by emailing me at emma.heath@iappanz.org.

I hope that access to these additional privacy resources will be of benefit to your work as a privacy professional.

Increase in membership fees from 1 August 2015

Please note that, as advised in our previous edition of Privacy Unbound, iappANZ has introduced a membership fee increase and a new tiered fee structure as of 1 August 2015. More details are on page 23 of this issue of the journal. Please email admin@iappanz.org if you have any membership queries.

Emma Heath, iappANZ General Manager

Visit our website, join us on LinkedIn or follow us on Twitter

To join the privacy conversation, keep up to date on developments and events and to make connections in your professional community, connect with us today!

Our website is www.iappANZ.org.au. You can log in to our member area from our website homepage with your email and password to access past bulletins. You can also get a new password or be reminded of your username if you have forgotten it. Just click on the links on the log in box. If you still need help email us at admin@iappanz.org.

Our LinkedIn group is: 
http://www.linkedin.com/groups?gid=1128247&trk=anetsrch_name&goback=.gdr_1281574752237_1

Follow us on Twitter at: https://twitter.com/iappANZ
Bradley Cooper’s taxi ride: a lesson in privacy risk

by Anna Johnston

Hollywood heartthrob Bradley Cooper is a bad tipper. That was the conclusion drawn by media – though denied by his PR rep – when data about 173 million New York taxi trips became public.

But I drew a different and more disturbing conclusion, which was how easy it is to get privacy ‘wrong’, when a government official is trying to get transparency ‘right’. Here’s what happened.

In March 2014, the New York City Taxi & Limousine Commission (known by the rather sweet acronym TLC) released under FOI data recorded by taxis’ GPS systems. The dataset covered more than 173 million individual taxi trips taken in New York City during 2013. The FOI applicant used the data to make a cool visualisation of a day in the life of a NYC taxi, and published the data online for others to use.

Top marks for government transparency, useful ‘open data’ for urban transport and planning research … but not, as it turns out, great for Bradley Cooper.

Each trip record included the date, location and time of the pickup and drop-off, the fare paid, and any recorded tip. It also included a unique code for each taxi and taxi driver.

In theory the identity of each taxi and taxi driver had been ‘anonymised’ by the use of ‘hashing’ – a one-way encryption technique which replaced each driver licence number and taxi medallion number with an alphanumeric code, that can’t be reverse-engineered to determine the original information.

However as a computer scientist who found the published dataset pointed out, hashing is not a good solution when you know what the original input might have looked like. So if you know what taxi numbers look like (and that’s not difficult - they are printed on the side of the taxi), you can run the ‘hash’ against all possible taxi numbers. It took a software developer less than an hour to re-identify each vehicle and driver for all 173 million trips. So anyone can now calculate any individual driver’s income for the year, or the number of miles they have driven, or where they were at any given time. So much for their privacy.

But what’s this got to do with Bradley Cooper, you ask?

Geolocation data exposes behaviour

While the computer science community started debating the limits of hashing and how TLC should have ‘properly’ anonymised their dataset before releasing it under FOI, an astute postgrad student found that even if TLC had removed all the details about the driver and the taxi, the geolocation data alone could potentially identify taxi passengers.

To demonstrate this, Anthony Tockar googled images of celebrities getting in or out of taxis in New York during 2013. Using other public data like celebrity gossip blogs, he was able to determine where and when various celebrities got into taxis. Using the TLC dataset, Anthony could then identify exactly where Bradley Cooper went, and how much he paid. (Mind you, cash tips are not recorded, hence the debate about whether or not he is a bad tipper.)

Anthony also developed an interactive map, showing the drop-off address for each taxi trip which had begun at a notorious strip club. I imagine the same could be done to easily identify the start or end-point for each taxi trip to or from an abortion clinic, a drug counselling service, or the home address of an investigative journalist, suspected whistle-blower or partner suspected of cheating.

As Anthony notes, “with only a small amount of auxiliary knowledge, using this dataset an attacker could identify where an individual went, how much they paid, weekly habits, etc … ‘I was working late at the office’ no longer cuts it”.
Open data or open sesame?

The publication of the NYC taxi dataset illustrates a particular challenge for privacy professionals: how easily an individual’s identity, pattern of behaviour, physical movements and other traits can be extrapolated from a supposedly ‘anonymous’ set of data, published with good intentions in the name of ‘open data’, public transparency or research.

Other recent examples have included the re-identification of ‘anonymous’ DNA donors to the ‘Thousand Genomes Project’ research database, and the re-identification of bike riders using London’s public bicycle hire scheme. As the blogger who turned the publicly available bike trips dataset into interactive maps noted, allegedly ‘anonymous’ geolocation data, even when months old, can allow all sorts of inferences to be drawn about individuals – including their identity, and their behaviour.

Closer to home, the NSW Civil & Administrative Tribunal has shown they are willing to challenge, rather than blindly accept, assertions by government agencies about the identifiability of data, by accepting that if a "simple internet search" links the data in question back to an individual’s identity, the published data will meet the definition of ‘personal information’, and its publication or disclosure becomes contestable under privacy law.

For privacy professionals, the goalposts are shifting. An assumption that data has been ‘de-identified’, and is thus not subject to privacy restrictions, may no longer hold true.

Privacy Officers would do well to engage with their colleagues who might publish or release datasets, such as people working in FOI, open data, corporate communications or research, to ensure they understand the risks of re-identification, and know about their disclosure obligations under privacy law.

You don’t want your ‘open data’ to become ‘open sesame’.

Anna Johnston is Director, Salinger Privacy

Salinger Privacy provides specialist privacy consulting and training services. Salinger Privacy publishes a blog, as well as eBooks on privacy law, including an annotated guide to the NSW privacy laws. Find Salinger Privacy at www.salingerprivacy.com.au
Privacy and data protection in Victoria: Q&A with David Watts

Recently, we put some questions to David Watts, the inaugural Commissioner for Privacy and Data Protection in Victoria, Australia.

Before being appointed as Commissioner in 2014, David was the Commissioner for Law Enforcement Data Security and the Acting Privacy Commissioner for Victoria. Prior to this he was Assistant Secretary, Legal Services Branch, of the Department of Health and Ageing in Canberra where he led the development of the regulatory framework to support national e-health initiatives and the national registration and accreditation scheme for the health professions. Before that, he headed the legal branch of the Victorian Department of Human Services where he was closely involved in the development of key social policy-based legislative initiatives including the Children, Youth and Families Act 2005.

Privacy Unbound co-editor Veronica Scott asked David the following questions:

How did you become a privacy professional?

I’m not sure that I am a privacy professional! My background is as a lawyer who has practised in both the private and public sectors specialising in information technology, information privacy, intellectual property, governance and regulatory systems.

In the mid-1990s I did a lot of technology-related legal work and became interested in internet law issues. I acted for a number of pioneering internet-based technology organisations. Privacy was one of the issues that was becoming increasingly relevant to the way they operated. Becoming involved with privacy was incidental to my interests in content and technology.

Can you describe your role as the inaugural Commissioner for Privacy and Data Protection?

The most simple (and boring) answer to this question is to read s103 of the Privacy and Data Protection Act 2014 (PDPA).

The Commissioner for Privacy and Data Protection needs to provide thought leadership in the fields of information privacy and security for the Victorian public sector. My role needs to engage in contemporary information issues identified through multi-disciplinary research capabilities, and provide practical guidance material as an output.

Can you explain for our readers the key changes to the Victorian Privacy and Data Protection Act 2014 introduced when it replaced the Information Privacy Act (IPA) 2000?

Uniquely, the old IPA omitted any mechanism that permitted public interest departures from the Information Privacy Principles (IPPs). The new legislation contains provisions that permit departures from (most) of the IPPs if there is a substantial public interest in doing so.

Also uniquely, the PDPA empowers the development of protective data security standards that are backed by law. The standards will apply to all Victorian government information (with a few health-related exceptions).

What are the current issues in privacy and data security that your office is working on/researching?

My key priorities for the first 18 months as the Commissioner for Privacy and Data Protection Develop are as follows:

- Develop and issue the Victorian Protective Data Security Standards
• Develop, monitor and implement an assurance system for privacy and data security
• Strengthen the security of law enforcement data
• Build effective and collaborative stakeholder relations
• Provide thought leadership in emerging privacy and data security issues (eg Privacy by Design, Security by Design, Big Data, Public sector information sharing, Cloud computing)

*How do you rate Australia and Victoria in particular in relation to privacy rights and protections?*

Overall Australia rates fairly poorly. There reason for this is the very limited application of the private sector provisions of the Commonwealth Privacy Act 1988.

*How are Victorian agencies implementing privacy by design (PbD) in their organisations?*

Organisations can implement PbD in a number of ways, from a project-by-project approach or a full rollout approach.

Optimally, PbD should be implemented across an entire organisation. However, in practice, implementation may initially occur on a project-by-project basis. In a case study conducted jointly by the Canadian Privacy Commissioner and IBM, it was suggested that it may be wise to 'start small, learn and expand.' A project-by-project approach nevertheless carries the risk that in the long term, a specific process or project may be privacy-protective but the entire organisation may not be. A project-by-project approach should be seen as an interim step to a full rollout of PbD.

Some of the most useful tools that can be used to implement PbD are Privacy Impact Assessments and Security Incident Management.

*Do you agree that there should be mandatory privacy breach reporting and if so why?*

Yes, for two main reasons. First, breach reporting serves to hold organisations to account. Secondly, breach reporting helps us learn from our mistakes.

*Please describe the key privacy issues faced by CPDP and its clients over the past year. Are there particular trends that you have observed in 2014?*

Analysis of the complaints and enquiries received by CPDP reveal that surveillance and tracking of individuals through electronic devices continues to be a significant concern to the community.

This concern appears to coincide with the escalating use of Closed Circuit Television (CCTV) at private residences and within the workplace. Additionally the common use of CCTV and Global Positioning Satellite (GPS) technology by organisations to conduct surveillance on employees continues to be an issue. These and other surveillance and tracking technologies, such as smart phones used to covertly record conversations, can undermine the notion of anonymity and a right to privacy free from government and corporate interference.

*On a more personal note – can we ask you what music you like and what books you are reading?*

I decided to learn guitar properly a few years ago and I’ve become fond of Lightning Hopkins blues songs. I’ve just learnt ‘Hard Times Killing Floor’ blues and am just starting on his version of ‘Baby, Please Don’t Go’. In the process, I’ve become a bit of a guitar nerd. I’m practicing on an old 1948 Gibson ES 150 (the same type that Billy Bragg uses on the cover of Tooth and Nail).

I’m reading ‘The Peripheral’ by William Gibson. Other books I’ve enjoyed this year include the ‘Book of Numbers’ by Joshua Cohen and ‘A Field Guide to Getting Lost’ by Rebecca Solnit.

David Watts is the Commissioner for Privacy and Data Protection in Victoria

Veronica Scott is Special Counsel at Minter Ellison Lawyers, an iappANZ board member and co-editor of Privacy Unbound
Big Data, Ethics and Privacy in Human Research

by Jodie Mcvernnon, Deborah Warr and Assunta Hunter

Introduction

The ever-increasing capacities of digital technologies to collect, replicate and store information are transforming the ways in which research is conducted. They also are introducing new kinds of ethical issues for researchers to grapple with.

Digital data includes information that is routinely collected within research protocols. Individuals are also using various devices that ‘emit’ information that becomes research data, including metadata. Increasingly individuals providing information may not be aware that there are expanding capacities for their information to be ‘harvested’ for research, as well as having considerable commercial value. It is not always possible to specify the ways in which information may be ‘repurposed’ and analysed into the future.

Varied digital data also have enhanced capacities to be linked at individual or geospatial levels providing opportunities for interdisciplinary research addressing a range of complex social, economic, health, environmental and other issues. The emerging possibilities for research must be tempered by awareness of arising ethical issues, including risks that are presented to individual privacy and confidentiality.

Privacy, confidentiality and consent

While privacy is a legal issue and there are provisions aiming to protect individuals’ privacy when required to provide certain kinds of information, research using digital data can present risks to participants’ privacy and confidentiality that must be carefully considered. Ethical issues are associated with questions of consent to participate in research, assessing the potential benefits of research and promoting awareness in the community that digital data may be used in research.

Where consent for data collection has been obtained for the purposes of research, plain language statements provide individuals with reasonable expectations about the use of their information. The potential for data to be reused complicates these processes. Researchers and data custodians must balance issues of extracting the most value from data collected through publicly funded research and ensuring participants’ privacy and confidentiality is maintained. Developing community consensus for assessing these competing benefits and risks can be difficult. Even the use of health information without consent, for which there may be a clear public health benefit, is controversial.

Capacities to ‘de-identify’ data are used to maintain individual privacy at the same time other possibilities of digital data, location referencing and linkage of data sets, present new risks that participants may be identified. In Australia, researchers have successfully implemented a variety of technological approaches to address these issues, including strategies for obfuscating geo-spatial data statistical disclosure control and the use of remote analysis servers, but they are currently inconsistently applied.

The case for revised guidelines for research involving digital data

The National Statement on Ethical Conduct in Research (2014), originally published in 2007, guides the conduct of research involving human participants in Australia. At this time, it did not anticipate the expansion of research involving digital data, including data linkage and the increasingly interdisciplinary and international nature of research.

Without adequate ethical guidelines researchers must navigate these issues in piecemeal fashion, ethics committees are hampered in assessing ethical risks and the suitability of measures to minimise risks, the interests of research participants are not fully protected and public trust in research may be compromised.

Internationally relevant guidelines to guide ethical research conduct research in this area are urgently needed.

To promote this process, we engaged with a broad cross-disciplinary and cross-sectoral group to develop a consultation document, with funding support from the Carlton Connect Initiative at the University of Melbourne. The Guidelines for the Ethical Use of Digital Data in Human Research can be accessed at: http://www.carltonconnect.com.au/area/pervasive-it/.
The Guidelines identify five categories of key ethical issues for researchers and human ethics committees: (a) Consent; (b) Privacy and confidentiality; (c) Ownership and authorship; (d) Data governance and custodianship and (e) Data sharing and assessing the social benefits of research. In this context, the Guidelines pose questions that should be considered when conducting research involving digital data, and also questions for members of human research ethics committees who are reviewing projects involving the use of digital data.

From a privacy perspective, the questions that the Guidelines suggest should be asked are by researchers and ethics committees are:

- Does the data in question constitute personal information in the sense of the Privacy Act?
- Is there any mechanism, regulatory framework or administrative structure that is designed to protect the individual’s privacy in relation to the project?
- Does the creation of data in this project challenge individual or community expectations about privacy?
- If explicit consent has not been obtained for this usage of data, does the public interest, as laid out in the NHMRC National Statement on Ethical Conduct in Human Research (2007), support its use without consent?
- To what extent are the data gathered in this context considered personal and private, or public and available for research purposes?

The Guidelines are a consultation document, and we would be delighted to receive comments from readers of Privacy Unbound.

Associate Professor Jodie McVernon heads the Modelling and Simulation Unit within the Centre for Epidemiology and Biostatistics, Melbourne School of Population and Global Health at the University of Melbourne.

Associate Professor Deborah Warr is a VicHealth Research Fellow with the McCaughey Centre at Melbourne School of Population and Global Health at the University of Melbourne

Dr Assunta Hunter has recently completed a PhD in medical anthropology at the University of Melbourne.
What’s on the privacy agenda for the Office of the Australian Information Commissioner?

By Timothy Pilgrim, with Melanie Marks

This month we continue our regular series of Questions and Answers with the Australian Privacy Commissioner (and Acting Australian Information Commissioner) Timothy Pilgrim:

The future of the OAIC continues to garner media attention. Can you shed some light on the current status of the OAIC and how you see the Office operating through the mid to longer term?

When the Government announced its intention to establish new arrangements for the OAIC’s functions, we began readying for that change by transferring our FOI complaints to the Commonwealth Ombudsman and our FOI policy and reporting functions to the Attorney-General’s Department. The Bill to abolish the OAIC would also see FOI Information Commissioner (IC) Reviews being dealt with by the AAT. However, the Bill required to effect that change has not been considered by the Australian Senate.

As a result, some funding was reappropriated to allow the OAIC to continue with a streamlined IC review processes. This was in addition to the funding already allocated for our privacy work, as well as some new funding provided to allow the OAIC to undertake oversight activities in regard to some privacy aspects of the new national security legislation.

This situation has created uncertainty and speculation, particularly amongst administrative law and open government advocacy circles, about the status of the OAIC and the important role that it performs for the community in the privacy and FOI spaces.

However, we have not allowed this uncertainty to hold us back from fulfilling our responsibilities, and we have achieved an incredible amount over the last 12 months, in both privacy and FOI. For example, one of our deliverables for the 2014–15 year was to finalise 80% of privacy complaints within 12 months. However, we achieved 98.3%, a remarkable improvement on last financial year.

So, my message for organisations and agencies is — don’t get complacent about your privacy responsibilities, or about the capacity of the OAIC to do its job in ensuring the community’s rights are upheld under both the Privacy Act and the FOI Act.

You’ve recently highlighted that “strategic privacy assessments” are a key focus of the Office going forward. Can you tell us more about what these will entail? How will you choose which entities to review?

With the privacy law reforms of 2014 having been in place now for eighteen months we’re moving our focus to helping entities ensure they have the right privacy governance frameworks in place, and assessing how entities are complying with their privacy obligations.

Privacy assessments are essentially a point-in-time snapshot of how well an entity is managing their privacy obligations in a specific area. Assessments are a collaborative process where we work with an entity to identify specific or potential problems with information gathering, handling or management. At the end of that process we are able to give recommendations and advice on how to improve in any problematic areas.

The OAIC has undertaken a risk targeting exercises to identify assessments for 2015–16 which will contribute to achieving the goal of promoting and ensuring the protection of personal information. Some of the targets are chosen primarily to assess how systems and processes are being developed to implement new legislation which have privacy impacts, and others because an industry or technology affects the privacy of a large section of the community.

APP 1 privacy policies are an area that we have, and will continue, to target, in a variety of sectors. In addition to this, in the 2015–16 year we will be working with the Department of Immigration and Border Protection on a number of assessments, including on its collection of biometric and other information at airports. We will also assess a number of telecommunications service providers, including on how they are protecting data retained under the mandatory data retention scheme. And in the health sector we will continue to assess private and public sector entities in relation to the protection of personal information when using the eHealth
system. Other assessments will include an ACT government department, users of the Document Verification System and private sector and government entities not previously assessed by the OAIC.

Primarily, assessments aim to educate entities and ensure improvements through the implementation of OAIC recommendations. However, in some circumstances, for example where recommendations are not taken on board, the OAIC may take further regulatory action as a result of an assessment.

*Your determination in Ben Grubb v Telstra Corporation Limited is awaiting appeal before the AAT. What approach should organisations take whilst we await the outcome?*

In finding that Telstra had breached the Privacy Act in refusing to provide Ben Grubb with his metadata, I had to first conclude, against Telstra's argument, that Mr Grubb's metadata did in fact constitute personal information.

Telstra argued that much of the metadata sought was simply not 'personal information', because on its face the data was anonymous. This is correct. But that argument overlooks the reality of data-linking and that a customer's identity and much more information about them can be established by cross-matching data sets. Personal information is not just that which does identify you but also that which reasonably can.

For this reason the challenge faced by Telstra will lie with any organisation that handles complex data sets in which anonymous data can be linked to other sources from which an individual becomes reasonably identifiable.

Pending any appeal outcomes, my advice to prudent organisations would be to work on the assumption that such data is "personal information" and to manage it and secure it as if it is.

*The International Conference of Data Protection & Privacy Commissioners is coming up in October in the Netherlands. What do you expect will be the key outcomes of the Conference?*

This year's International Conference will be concerned with a broad range of topics, with international cooperation and cross-border regulation high on the agenda.

At the October meeting, the International Conference will be introducing a new Global Cross Border Enforcement Cooperation Arrangement. This Arrangement states that "a global phenomenon needs a global response", and recognises that, when data protection issues arise, trans-border data flows can quickly affect the privacy of large numbers of individuals.

Taken in conjunction with updates to the APEC Privacy Framework, the appointment of an EU Special Rapporteur for Privacy, and a new EU regulation on mandatory data breach notification (updating the EU Directive), it is clear that global cooperation on privacy and data protection will be a central feature of modern enforcement trends in regulating international data flows and trans-national companies.

Timothy Pilgrim is the Australian Privacy Commissioner and the Acting Australian Information Commissioner.

Melanie Marks is Vice President of iappANZ.
From sex, lies and video tapes to class actions: the hidden world of privacy litigation

by Emma Hossack

If you think the remedies for privacy breach are trivial in the absence of a formal tort for invasion of privacy in Australia – you can think again.

In 2015, both ISACA and the Centre for Media and Communications Law / Gilbert+Tobin Lawyers hosted witty and thought provoking presentations by Michael Rivette, a Melbourne-based barrister who specialises in privacy litigation.

Here are just a few of the highlights about the treacherous waters of privacy litigation. You can hear more directly from Michael at the iappANZ Privacy@Work Summit in Melbourne on 18 November 2015.

Privacy litigation is happening

We have all heard the complaint that the current legal framework for privacy protection simply fails to attract any serious penalties. Even the fines and remedies available under the amended Privacy Act 1988 seem insignificant compared to the damage that breaches can cause. Such damage can be particularly extreme if you take the view of Professor Luciano Floridi1, that information about you - such as your genetic code, memories, and beliefs - is just as much a part of you as say your left arm. But wherever you sit in the current philosophical and legal debates about the ‘right to be forgotten’, the right to control your personal data and the importance of privacy versus the public’s ‘right to know’, all must acknowledge the harm to individuals that can be caused by privacy breaches.2

What we learned from Michael’s presentations is that there are plenty of privacy cases being litigated right now. You might be surprised to read this – as if this is a lively area for litigation, where are the stories and why haven’t you read anything in the newspapers?

The answer is that the first thing good legal practitioners do when litigation is commenced is to throw a blanket over the action and obtain a suppression order. So don’t be lulled into a sense of false security – privacy related actions are happening all the time and the emergence of class actions are of particular significance.

What sort of privacy litigation? Are we in chartered or unchartered waters?

Potential actions available under a range of statutory regimes might be the expected path or the “chartered waters”.

Depending on the nature of the matter and how an individual’s privacy was invaded, there are potential causes of action under surveillance devices legislation (at the federal and state levels), under privacy legislation (including the state regimes that regulate health privacy, and possible injunctions), under the Crimes Act and even under the Competition & Consumer Act – particularly if the person collecting the information has engaged in misleading or deceptive conduct.

If as a plaintiff, you plead a mixture of these and then include some equitable claims in the mix too – that’s when it can get really interesting.

Equitable actions are the more treacherous waters; these can be dangerous if you don’t know the risks – particularly in the area of costs. But equitable claims such as breach as confidence can be used to protect an individual’s privacy if it can be established that the

1 Professor of Philosophy and Ethics of Information at the University of Oxford, Oxford Internet Institute. Also chosen by Google for the Advisory Panel to assist it with its work in respect of the ‘right to be forgotten’ following the Court of Justice of the European Union ruling 13 May 2014, see http://www.theguardian.com/technology/2014/nov/13/right-to-be-forgotten-more-questions-than-answers-google

relevant information is confidential, that duties of confidence were owed, and there was damage.\(^3\) A relatively recent example of this is the "Giller case"- also known as the sex, lies and videotape case, which Michael successfully argued.\(^4\)

There are also a range of other potential weapons and causes of actions in a privacy plaintiff’s arsenal, including reliance on the laws relating to:
- copyright - particularly if the matter involves photographs, recordings or other works;
- trespass and nuisance;
- defamation;
- harassment / intentional infliction of harm

In addition, class actions are probably the most exciting for litigation lawyers and frightening for companies.

For instance, there is currently a representative action underway involving 9250 individual breaches or invasions of privacy. If each was awarded a relatively 'token' damages payment of $1,000, that would amount to a total of $9.25 million. Time will tell how this case concludes, but having regard to the nature of the personal information involved and all the circumstances (noting that the breach occurred due to a mistake), a payment in the vicinity of $5-6000 per breach would not seem out of the question, and that would total $46.25 million.

So now it’s serious money and not simply a theoretical human right we are looking at, what are some of the lessons that should be learned?

**Lessons to learn**

1. Be vigilant about how you treat personal information even if it was obtained in a public location (like the photo of Naomi Campbell leaving a drug rehabilitation clinic, in the famous case of *Campbell v Mirror Group Newspapers Ltd*).\(^5\) Also note the new laws being proposed in New Zealand, prompted by the fact that a couple who were videotaped having sex in an office (in full view of people in a pub across the road, who filmed them and posted the footage on social media) are unlikely to have any legal remedies because they did not take steps to ensure their privacy. As reported at the time, under the New Zealand crimes legislation, if a person is in a place where there is no reasonable expectation of privacy, a crime has not been committed.\(^6\)

2. Be aware of the terms when “trading” personal information in exchange for a good or service – such as obtaining a credit card or buying goods on line. There are parameters about what is reasonable as a term of trade.

3. Stop thinking about data as an asset only, and start thinking about your company’s information as information a human being allowed you to use. You hold personal information by licence.

4. It’s the individual’s personal reaction that matters – and how the relevant action impacted them personally. It’s not relevant if you think their reaction to your conduct (and how you have used or disclosed their personal information) is over the top. When applying remedial legislation, Courts will place weight on the interpretation of, and effect on, the person whose personal information has been disclosed.

---

\(^3\)The High Court case of *ABC v Lenah Game Meats Pty Ltd* (2001) 208 CLR 199 confirmed that plaintiffs needed to show that the information was confidential, imparted in circumstances of confidentiality and had done some damage. The joint judgement of Gummow and Hayne JJ in Lenah Meats paved the way for using breach of confidence actions to seek redress for breaches of privacy.


5. If you are facing an action under the Privacy Act – try to resolve it before the Privacy Commissioner. Going to the Federal Court will mean the possible imposition of high costs orders. The same applies where injunctions are involved.

6. Intention may be irrelevant – if you breach because you haven’t taken enough care – that is what the Courts will focus on.

7. If personal information is given for one purpose, don’t use it for another unrelated purpose without the consent of the individual.

8. Take your obligations seriously. Undertake audits and check your processes.

Michael Rivette gives a superb presentation. I am looking forward to hearing and learning more in November.

Emma Hossack is an iappANZ Board director, CEO of Extensia (a shared electronic health record company) and also CEO of Binder (an information logistics and storage platform). Emma is also the Vice-President of the Medical Software Industry Association and the former President of iappANZ
True Confessions: international and local developments in mandatory data breach reporting

By Carolyn Lidgerwood

On 3 March 2015, the then Australian Minister for Communications and the Attorney-General issued a joint media release¹ that signaled that a mandatory data breach reporting regime would be introduced this year in Australia. Specifically, in response to a recommendation by the Parliamentary Joint Committee on Intelligence and Security (in relation to then-draft metadata retention legislation), the media release stated:

_The Government agrees to introduce a mandatory data breach notification scheme by the end of 2015, and will consult on draft legislation._

This is not the first time that mandatory data breach reporting has been on the Australian political agenda, with the Privacy Amendment (Privacy Alerts) Bill 2013 previously having been introduced into the Parliament but lapsing at the end of 2013.²

Mandatory data breach reporting is also on the legislative agenda in New Zealand, albeit in the longer term, with a possible ‘two tiered’ level of privacy breach reporting being anticipated as part of the reform of the Privacy Act.³

Local developments in their global context

These ‘local’ developments with respect to mandatory data breach reporting are not happening in a vacuum. In the leading data privacy jurisdictions of Canada and the European Union, mandatory data breach reporting obligations are being introduced.

This article is intended to update readers of the developing situation in Canada and the European Union, for comparison with developments in Australia and New Zealand as they unfold.

What this article won’t try to do is to try to summarise the complex patchwork of State data breach notification laws that apply in the United States of America (49 at last count).⁴ While the USA could be said to have led the way in the mandatory breach reporting area, the sometimes-narrow approach to what amounts to ‘personal information’ make the USA States’ approach of less comparable interest for us in this part of the world, even if the underlying motivations for these laws are similar to those in other jurisdictions (ie the protection of individuals from fraud, identity theft and other serious harm).

Also, this article is should not be taken to suggest that reporting of serious data breaches is not expected now. Privacy and data protection regulators around the world (including in Australia, New Zealand and the United Kingdom) strongly encourage voluntary reporting in specified circumstances.⁵

However the new legal developments in Canada and the EU, and subsequently in Australia and New Zealand, will make data breach reporting enforceable.

---

¹ The media release was issued in response to the inquiry of the Parliamentary Joint Committee on Intelligence and Security into the Telecommunications (Interception and Access) Amendment (Data Retention) Bill 2014. Recommendation 38 of that report was that ‘The Committee recommends introduction of a mandatory data breach notification scheme by the end of 2015’.
² The Bill was re-introduced by the Opposition in 2014, but appears to have been stalled. See http://www.aph.gov.au/Parliamentary_Business/Bills_Legislation/Bills_Search_Results/Result?bId=s958
Canada

Recent amendments to the federal *Personal Information Protection and Electronic Documents Act* (PIPEDA) will require notifications to be made to the Canadian Privacy Commissioner (and potentially also impacted individuals) if a data breach occurs in a PIPEDA regulated area. The Canadian requirements have not yet come into force, as implementing Regulations are pending. Below is a summary of what is known as at the date of writing.

What is the reporting threshold?

In Canada, a regulated organisation is required to notify the Commissioner of ‘any breach of security safeguards involving personal information under its control if it is reasonable in the circumstances to believe that the breach creates a **real risk of significant harm** to an individual’.

Meaning of key terms

Under the Canadian legislation, a ‘breach of security safeguards’ means the loss of, unauthorised access to or unauthorised disclosure of personal information resulting from a breach of an organisation’s security safeguards or from a failure to establish those safeguards. This reflects familiar concepts to what we would understand to be a data security breach in Australia and New Zealand.

The term ‘significant harm’ is defined to include ‘bodily harm, humiliation, damage to reputation or relationships, loss of employment, business or professional opportunities, financial loss, identity theft, negative effects on the credit record and damage to or loss of property.’ This is both an expansive and inclusive definition.

In determining whether there is a ‘real risk’, the legislation identifies some relevant factors. Canadian organisations will need to consider the sensitivity of the impacted personal information and the probability that the personal information has been, is being or will be misused. That is helpful as it allows controls such as encryption to be taken into account (eg if an encrypted laptop is stolen).

When must the notification be made?

Such report must be made 'as soon as feasible after the organisation determines that the breach has occurred'. This appears to be a more pragmatic approach than prescribing arbitrary timelines (more on that below).

Does anyone else need to be notified?

In addition to notifying the Commissioner, organisations regulated under PIPEDA will also be required to notify the impacted individuals (again, if is reasonable to believe that the breach creates a real risk of serious harm), and also potentially other organisations if those other organisations may be able to reduce the risk of harm that could result from the breach.

Is there a particular form in which notifications must be made?

The forthcoming Regulations are anticipated to prescribe the form of reports to the Commissioner, and possibly also additional requirements for notifications to individuals. In relation to notifications to individuals, the requirement is for the notification to ‘contain sufficient information to allow the individual to understand the significance to them of the breach and to take steps, if any are possible, to reduce the risk of harm that could result from it or to mitigate that harm’.

What is the penalty for not notifying?

There will be penalties for ‘knowingly’ breaching the notification requirements of up to CAD $100,000 per incident.

---


7 PIPEDA does not ‘cover the field’ with respect to the Canadian private sector; for Constitutional reasons it applies to federally regulated organisations (eg in the broadcasting and communications and transport sectors) and to personal data that flows across provincial or national borders in the course of commercial transactions; but it won’t apply to private enterprises in provinces that have privacy legislation that has been held to be ‘substantially similar’ – eg Quebec. For more details see the Privacy Commissioner’s website at [https://www.priv.gc.ca/](https://www.priv.gc.ca/)
Are there other related requirements?

Regulated Canadian organisations need to keep and maintain a record of every ‘breach of security safeguards’ (or a ‘breach log’) and the Commissioner can request access to such records.

As noted, more details about the new Canadian laws will become known when implementing Regulations are published.9

European Union

Under the current EU Data Protection Directive 95/46/EC (as implemented into the national laws of EU member states), there is currently no general, mandatory data breach reporting scheme. Some EU member states have independently implemented mandatory personal data breach reporting obligations (eg the Netherlands is presently introducing such requirements)10, and there are some sector-specific laws requiring reporting (eg in the telecommunications sector) but this is not driven by the current Data Protection Directive.

As in Australia and New Zealand, data protection authorities in many EU member states strongly encourage voluntary reporting of serious data breaches. This will become mandatory when the proposed new EU General Data Protection Regulation (GDPR) becomes law. Specifically, the proposed new GDPR will require notification to the relevant Supervisory Authority (ie the data protection authority of the relevant member state) and the impacted individuals. The following summary is based on the version of the draft GDPR that was available as at the date of writing.11

What is the reporting threshold?

The relevant Supervisory Authorities and affected individuals must be notified of breaches that are likely to result in a ‘high risk for the rights and freedoms of individuals’. The reference to ‘high risk’ is significant as it qualifies the obligations (as discussed below).

Meaning of key terms

Under the draft GDPR, ‘personal data breach’ means a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, access to, personal data transmitted, stored or otherwise processed.

The term ‘high risk’ can be better understood when read in the context of proposed Articles 31 and 32, which requires notification of a personal data breach ‘which is likely to result in a high risk for the rights and freedoms of individuals, such as discrimination, identity theft or fraud, financial loss, unauthorised reversal of pseudonymisation, damage to the reputation, loss of confidentiality of data protected by professional secrecy or any other significant economic or social disadvantage’.

When must the notification be made?

Data controllers must notify the Supervisory Authorities of a personal data breach within 72 hours of becoming aware of it (where feasible). The 72 hour timeframe is extremely tight, but less so than the 24 hours that was proposed in earlier versions of the draft GDPR. If a data controller does not notify within that 72 hour time period, it will need to provide a ‘reasoned justification’ to the relevant Supervisory Authority.

Under Article 32, notifications to affected individuals/data subjects are required ‘without undue delay’.

What is the penalty for not notifying?

Under the draft GDPR, data protection authorities will have far stronger powers to impose fines for non-compliance. At the extreme, the maximum fine may be up to €1 million or, up to 2% of annual worldwide turnover, whichever is greater. However it should be

---

9 To monitor the progress of the Canadian developments going forward, see updates from Timothy Banks in the iapp Privacy Tracker at https://iapp.org/news/privacy-tracker
emphasised that sanctions are intended to be proportionate – and the Supervisory Authorities will have a ‘sliding scale’ of sanctions available (from warnings at the ‘lower end’ to heavy fines at the ‘upper end’).

Is there a particular form in which notifications must be made?

The Regulation prescribes the contents of the notification to the relevant Supervisory Authority. The report must:

- describe the nature of the personal data breach (including where possible and appropriate, the number and categories of data subjects and volume of data affected);
- specify the name and contact details of the data controller’s data protection officer (DPO) or other contact point;
- describe the likely consequences of the personal data breach;
- describe the measures proposed or taken to address the personal data breach, and
- where appropriate, indicate measures to mitigate the possible adverse effects of the personal data breach.

This is a lot to clarify within 72 hours.

There are similar requirements for reporting to individuals, with individuals needing to be informed of the nature of the data breach and ‘at least’ the details of the DPO or contact person and information about measures being taken to address the breach, and recommended measures to mitigate the possible adverse effects of the breach.

Are there any exemptions?

Under the draft GDPR, there are some important exceptions with respect to both notifications to individuals and Supervisory Authorities. For example, if the data controller has implemented security measures (in particular that render the data unintelligible to any person not authorised to access it, such as encryption) and those measures were applied to the data affected by the personal data security breach; or the data controller has taken measures to ensure that the ‘high risks’ are no longer likely to materialise, then notification is not required.

Are there other requirements?

As in Canada, the relevant organisation (data controller) is required to document personal data breaches (including the facts, the effects of the breach and the remedial action undertaken). In the EU, this documentation should be directed at enabling the Supervisory Authority to verify compliance.

What next for Australia and New Zealand?

The developments in Canada and the European Union illustrate that local moves towards a mandatory data breach reporting scheme are not occurring in isolation from the rest of the world.

Assuming that legislation is on the way in Australia and New Zealand, the challenge will be to ensure that the balance is right – ensuring that the reporting threshold is set at a level that addresses the likelihood of harm, without imposing unreasonable and unworkable administrative and legal burdens. For instance, if the mandatory notification threshold is set too low, then notifications to individuals can quickly become meaningless (as illustrated by the anecdotal evidence from the US about ‘breach fatigue’).12

From this writer’s personal perspective, the existing regulatory guidance from our regulators in Australia and New Zealand reflects a sensible approach. That should provide a useful starting point for the legislative drafters. If that type of approach is adopted, we can hope that mandatory breach reporting may not impose significant additional administrative burdens, and as Victoria’s Commissioner for Privacy and Data Protection observed earlier in this issue of Privacy Unbound, breach reporting will help us learn from our mistakes.

Carolyn Lidgerwood is Global Privacy Counsel at Rio Tinto, co-editor of Privacy Unbound and a board member of iappANZ.

---

iappANZ’s writing prize 2015: entries open

Entries remain open for this year’s writing prize for an article that is published in our monthly Journal editions from February to October 2015. Anyone can enter (you don’t have to be an iappANZ member), simply by writing and submitting an article between 500-1500 words that tells us something interesting, new and relevant about privacy.

All articles must be submitted by email, preferably in Word, to veronica.scott@minterellison.com, Carolyn.lidgerwood@riotinto.com or emma.heath@iappanz.org by 20 October 2015. We will need the author’s email address and contact number. You can submit as many articles as you like.

The winner will be announced at our Privacy Summit on 18 November 2015 in Melbourne and their name and details will be published on our website. We also hope to profile the winner in our Journal. So alert your network and get writing!

More details about the writing prize if you are interested:

- Our Editorial team, Veronica Scott and Carolyn Lidgerwood, plus President Anna Kuperman and Past President Malcolm Crompton, will decide on the winner whose article they judge to be the most interesting, original and relevant to our members.
- Some people won’t be eligible for the prize (sorry!). They are: iappANZ board members, contractors and employees and their family members.
- After the winner is announced we will notify them and arrange for the prize to be delivered to them if they are unlucky enough not to be at our Summit.
- There will (sadly) be one prize only. Its value is AUS$250, so that’s pretty good really.
- We may need to verify the winner’s identity so we don’t give the prize to the wrong person.
- If the prize is not claimed for any reason (and we hope this won’t happen) the author of the runner-up article as judged by the Editorial team will receive the prize.

To make sure things go smoothly and fairly (and we are sure they will) we just have to say that our decision in relation to any aspect of the award of the prize, including the content and publication of submitted articles, is final and binding and not up for discussion.
Employment opportunities for privacy professionals

News about employment opportunities is provided as a service to iappANZ members. If you would like a notice about employment opportunities at your organisation published in Privacy Unbound, please contact our editors (see details on last page).

Privacy and Security Advocate, Asia Pacific, Middle East, Africa and Russia
Hong Kong

For immediate consideration, please send a text (ASCII) or HTML version of your resume to jobs@google.com. Important: The subject field of your email must include Privacy and Security Advocate, Asia Pacific, Middle East, Africa and Russia - Hong Kong.

As a member of Google's Public Policy team, you help shape various product and issue agendas with policy makers inside and outside government. In addition, you will help advise our internal teams on the public policy implications of their products, working with a closely coordinated and cross-functional global team. The role requires significant experience either working with or in government, politics or a regulatory agency as well as an ability to grasp complex technical and policy issues.

Responsibilities

- Develop and lead public privacy and security campaigns policy goals that benefit Google's users, our business and the wider web
- Engage directly with politicians and policy-makers and support country teams on their interactions with them
- Build a network of trade associations, industry partners, non-profit groups and others to support policies that will help create/maintain a user-focused online environment as well as an open Internet
- Monitor and research current and relevant emerging policy issues
- Work cross-functionally to develop policy positions for review by Google's Policy, Legal, and Management teams

Minimum qualifications

- BA/BS degree or equivalent practical experience.
- Experience in politics including time spent working on campaigns or in government.
- Privacy and security experience.

Preferred qualifications

- Strong political and analytical skills.
- Familiarity with Internet technologies and the surrounding policy environments.
- Team player with a sense of humour and the ability to exercise good judgment in a rapidly changing and sometimes stressful environment.
- First-rate written and verbal communications skills.
Area
Technology moves quickly, so it's important that we work closely with politicians, regulators, academics and third parties around the issues that affect the Internet and our users. We advocate for Google on the big public policy issues of the day and often play a part in high-profile debates. In this role, you’ll combine creativity and intellectual rigor with the organizational skills to manage different campaigns and projects to tight deadlines. You’ll apply your expertise to real-world scenarios, acting as an inspiring advocate and enthusiastic team player eager to help shape the future of Internet and mobile policy.

Job details
Team or role: Marketing & Communications; Legal & Government Relations
Job type: Full-time
Job location(s): Hong Kong
Do you have solid experience working at a senior level within privacy management? If so, there’s an exciting opportunity to join Australia’s largest Infrastructure Project as part of nbn™’s Privacy and Security Knowledge Management team as a Senior Privacy Advisor. Read on for details!

**Senior Privacy Advisor**

**North Sydney location.**

**Your role in the future**

nbn is designing and building Australia’s broadband network – the largest technology program the country has ever seen. By 2020, 8 million happy homes and businesses will benefit from fast broadband on a network using a range of technologies.

This once in a lifetime nationwide program provides loads of opportunity, flexibility and exposure to a vast array of projects. It is a rare chance to shape yours - and Australia’s - future.

Reporting to the Head of Privacy and Security Knowledge Management, the Senior Privacy Advisor provides expert privacy advisory services to internal business customers. This role is also responsible for running and constantly improving the overall nbn privacy management framework.

The role requires excellent knowledge of the practical application of Australian privacy regulations and exceptional stakeholder management to ensure consistent and effective privacy outcomes. They will work in close collaboration with the existing Privacy team, wider Legal and Security Department and key stakeholders to ensure the privacy considerations are integral throughout the information lifecycle and in applicable nbn activities and projects.

**You can help us:**

- Ownership of privacy related policies, guidelines, management plans and reporting
- Acting as the trusted privacy advisor to deliver timely, accurate and effective privacy guidance to business stakeholders
- Performing Privacy Impact Assessments and third party privacy reviews
- Working closely with Corporate Risk Team to advise business owners on privacy related risks and controls
- Providing subject matter expert input into the Security and Privacy Education and Awareness program
- Conducting and co-ordinating assurance activities in conjunction with the wider security assurance team and other internal stakeholders

This is a great chance to broaden your skills and be part of something really big.
Your skills:

This is an excellent opportunity, one that requires a solid understanding of the privacy landscape. The Senior Privacy Advisor MUST be a self-starter, who can bring energy and enthusiasm to the Security Group and help the existing team to deliver and continually improve a first class privacy program.

With these skills you can help us deliver broadband to every part of the country:

- 8 – 10 years’ experience working at a senior level within privacy management or a very closely related field
- Excellent understanding of Australian privacy regulation and its applicability in a business environment
- A background in law, risk, compliance or security would be desirable
- Tertiary education or professional qualification in a related field preferred
- Experience working with risk management frameworks is also desirable

Your role in the future could start right here.

To apply, please submit an online application via nbn’s Careers site (see link below), including a brief covering letter with your resume, sharing relevant achievements for this position.

https://nbncojobs.taleo.net/careersection/external/jobdetail.ftl?job=200724402680

Applications close Friday 16th October, 2015

nbn is committed to the wellbeing of its employees and contractors and to enabling work to be performed in a productive manner that does not jeopardise one’s own safety or the safety of others. Employment with nbn is subject to pre-employment and on-going drug and alcohol testing as well as background checks, which may include service and pay history from your previous employment.
**Australian Government**

**Office of the Australian Information Commissioner**

**Assistant Director, Strategic Communications and Coordination**

**Regulation and Strategy Branch**

<table>
<thead>
<tr>
<th>Details</th>
<th>Location</th>
<th>Sydney</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Classification and Salary</strong></td>
<td>EL1 ($95,736 – $102,409 + 15.4% super)</td>
<td></td>
</tr>
<tr>
<td><strong>Type of Vacancy and Duration</strong></td>
<td>12 month maternity leave position</td>
<td></td>
</tr>
<tr>
<td><strong>Contact Officer for information</strong></td>
<td>Richard O’Neill, Director Stakeholder Engagement and Communications ( +61 2 8231 4260 )</td>
<td></td>
</tr>
</tbody>
</table>

**Email applications to:** [OAICjobs@humanrights.gov.au](mailto:OAICjobs@humanrights.gov.au)

**Closing Date for Applications** | 7 October 2015

**Applicant Information**

Thank you for your inquiry about working in the Office of the Australian Information Commissioner (OAIC). This document has been prepared to help you apply for this position. An order of merit may be created and may be used to fill subsequent positions or shorter term opportunities in this position. Any further job specific information required should be sought from the contact officer Mr Richard O’Neill, Director Stakeholder engagement and communications on +61 2 8231 4260.

**About the Office of the Australian Information Commissioner**

The OAIC is a statutory agency within the Attorney-General’s portfolio. The OAIC has regulatory functions under the *Privacy Act 1988* and the *Freedom of Information Act 1982* and is created by the *Australian Information Commissioner Act 2010*.

**Role: Assistant Director, Strategic communications and coordination**

The position is located in the Regulation and Strategy Branch, which delivers a broad range of strategic advice and regulatory functions. This is a unique environment in which the OAIC engages closely with both the public and private sectors.

The Assistant Director, Strategic communications and coordination will be responsible for providing strategic support to the Director and OAIC Executive on media management, communications and corporate reporting. This includes responsibility for maintaining and developing relationships with journalists, preparing and briefing Executive prior to media engagements, project managing elements of the OAIC’s communications activities including campaigns, events, social media, speeches and overseeing a range of corporate governance activities.

The Assistant Director, Strategic communications and coordination position is a key role within the OAIC and is the organisation’s primary media-facing role. The successful applicant will be a highly motivated team player who has experience in dealing strategically with media, preparing Senior Executives prior to media engagements, write for a variety of communications channels, and have the ability to work in a fast paced, small team environment.

**Duties:**

1. Advise Director and Executive on strategic engagement with media and other communications channels, including briefing Executive prior to interviews
2. Assist the Director with the OAIC’s engagement with international and domestic networks and fora
3. Preparation of media releases, statements, education materials, speeches, publications and other communications (including speech writing and internal communications)
4. Lead development and implementation of the OAIC’s communications strategy to reach the community, business and government sectors
5. Provide event management coordination for OAIC events such as Privacy Awareness Week
6. Oversight the production of reports and briefings including the OAIC Annual Report and other parliamentary and corporate governance requirements
7. Supervise staff in accordance with the OAIC’s performance management scheme
8. Other duties, consistent with above, as directed

Notes
- These duties are to be performed in accordance with the OAIC’s policies including the APS Code of Conduct and Values, Workplace Diversity and Work Health and Safety.
- Note that the successful candidate may be required to undergo a security assessment.

Selection criteria:
There are five core criteria for employment at the Executive Level 1 level, as listed below. Each criteria have associated capabilities which are indicative of the criteria. For more information regarding the core EL1 selection criteria and the associated capabilities please see the Australian Public Service Commission website at http://www.apsc.gov.au/publications-and-media/current-publications/resources/ils-el1-profile. The APSC’s work level standards for EL1s may also be of assistance: http://www.apsc.gov.au/publications-and-media/current-publications/worklevel-standards/el1

You should frame your application against the selection criteria outlined below, taking into consideration the duties of the position as well as the capabilities for the core criteria.

Core selection criteria
1. Shapes strategic thinking
2. Achieves results
3. Cultivates productive working relationships
4. Exemplifies personal drive and integrity
5. Communicates with influence

Job specific criteria
6. A sound understanding of privacy and freedom of information legislation; and of the role of statutory institutions, such as the Office of the Australian Information Commissioner, or the ability to quickly acquire.

Eligibility
Applicants must be Australian citizens, or be eligible for citizenship.

Terms and Conditions
Terms and conditions of employment will be in accordance with the OAIC’s Enterprise Agreement which can be found here: http://www.oaic.gov.au/about-us/corporate-information/key-oaic-documents/oaic-enterprise-agreement-20112014

General Information
Please read the information for job applicants on the OAIC website, which provides general information on applying for these positions. In that material you will find information about eligibility, the selection process, how to prepare a statement of claims and the Applicant Details form. Any further information required should be sought from the contact officer.

Applications should consist of the following:

- One page covering letter
- Resume or CV
- A statement against the selection criteria.
- Applicant Details Form (.doc) (.pdf)
Please note that the Australian Human Rights Commission administers the recruitment function for the Office of the Australian Information Commissioner.

Please send your application to the Human Resources Officer C/- Australian Human Rights Commission:

by email to: oaicjobs@humanrights.gov.au
or
by mail to: GPO Box 5218 Sydney, NSW, 2000

Selection Results: You will be advised of the outcome of the process by email.
Adviser, Regulation and Strategy

- Ongoing/non-ongoing, full-time/part-time positions available.
- APS Level 6
- Salary range: $75,965 - $83,652 + 15.4% superannuation.
- Location: Sydney
- Closing Date: 28 October 2015

See Applicant Information / About the OAIC in the previous listing

Advisers in the Regulation and Strategy Branch deliver a broad range of strategic policy and regulatory functions under the Commonwealth Privacy Act 1988. This is a unique environment in which the OAIC engages closely with both the public and private sectors.

Proactive regulatory work includes conducting assessments of privacy compliance of government agencies and the private sector, conducting Commissioner initiated investigations, providing advice on data breach notifications and preparing legislative instruments including Public Interest Determinations.

Strategic policy work includes developing guidance on privacy for, and providing advice to, government agencies and private sector organisations to help them understand and comply with their privacy obligations. It also includes examining government legislative and policy proposals that may have a privacy impact, including ehealth, identity management and authentication and national security initiatives. In addition, the Branch provides privacy policy advice under memorandum of understanding arrangements with government departments, and works with the private sector to ensure compliance particularly in the area of new technologies and legislative reform.

The Adviser is a highly motivated team player with the following attributes:

- ability to provide high quality strategic policy and regulatory advice on privacy law and issues
- ability to conduct investigations of potential privacy breaches, including gathering information from publicly available resources, making written and verbal inquiries and writing investigation reports
- ability to participate in privacy assessments (previously known as audits) of entities and write assessment reports
- high level analytical and conceptual skills
- awareness of new and emerging information technologies
- excellent communication and editing skills, including the ability to write clearly, in plain English and for different audiences
- strong organisational and project management skills
- the ability to turn ideas into action, and
- a keen eye for detail.
The Adviser, Regulation and Strategy will support Assistant Directors, Directors and the Assistant Commissioner of the Regulation and Strategy Branch to deliver services to the Commissioners, staff of the OAIC, government and the private sector.

Duties

1. Deliver high quality strategic policy and regulatory services to the OAIC, government agencies and private sector organisations on privacy law and issues.
2. Prepare guidance on compliance with privacy law and privacy best practice directed at the private sector, public sector, and individuals.
3. Conduct investigations of potential privacy breaches including gathering information from publicly available resources, making written and verbal inquiries and writing investigation reports.
4. Conduct assessments (previously known as audits) of privacy compliance and write assessment reports, including recommendations.
5. Analyse proposed regulatory initiatives and enactments to minimise any adverse effects on the privacy of individuals.
6. Prepare submissions in response to regulatory initiatives and enactments.
7. Prepare legislative instruments, including drafting and undertaking consultation.
8. Undertake complex policy and regulatory analysis and research, external and internal consultation and employ sound project management.
9. Promote awareness and understanding of privacy legislative requirements and assist agencies and organisations with their legislative obligations
10. Build sustainable and productive professional relationships with key stakeholders in the public and private sectors.
11. Other duties, consistent with above, as directed.

The precise duties of the successful applicant will vary depending on which team in the regulation and strategy branch they are placed. Applicants are encouraged to apply even if they only have relevant experience in some of the above areas.

Notes

- These duties are to be performed in accordance with the OAIC’s policies including the APS Code of Conduct and Values, Workplace Diversity and Work Health and Safety.
- Note that the successful candidate may be required to undergo a security assessment.
- Under section 25 of the Public Service Act 1999 the OAIC may re-assign the duties of an employee from time to time.

Eligibility

Applicants must be Australian citizens, or be eligible for citizenship. Relevant qualifications/experience in one or more of the following areas would be highly desirable: law, public policy, proactive regulation, information technology, editing, auditing, speech writing.

Position Location

This position is located in Sydney.

Terms and Conditions

Terms and conditions of employment will be in accordance with the OAIC’s Enterprise Agreement which can be found here: http://www.oaic.gov.au/about-us/corporate-information/key-oaic-documents/oaic-enterprise-agreement-20112014
General Information

Please read the information for job applicants on the OAIC website, which provides general information on applying for these positions. In that material you will find information about eligibility, the selection process, how to prepare a statement of claims and the Applicant Details form. Any further information required should be sought from the contact officer.

Applications should consist of the following:

- One page covering letter
- Resume or CV
- A statement against the selection criteria.
- Applicant Details Form (doc) (pdf).

Applications should be submitted by COB 28 October 2015.

Please note that the Australian Human Rights Commission administers the recruitment function for the Office of the Australian Information Commissioner.

Please send your application to the Human Resources Officer C/- Australian Human Rights Commission:

- by email to: oaicjobs@humanrights.gov.au;
  or
- by mail to: GPO Box 5218 Sydney, NSW, 2000

Selection Results

You will be advised of the outcome of the process by email.

Selection Criteria

There are five core criteria for employment at APS 6 level, as listed below. With each criterion, there is a list of related capabilities set out for your reference. These capabilities are indicative of the criteria and it is not intended that applications and assessments should address each and every capability. For more information regarding the core selection criteria, please see the Australian Public Service Commission website at http://www.apsc.gov.au/publications-and-media/current-publications/resources/ils-aps-6-profile

In addition, there are two additional job specific criteria for the position, as detailed at http://www.oaic.gov.au/about-us/careers/adviser-aps6-rs-september-2015

You should frame your application against the selection criteria outlined at http://www.oaic.gov.au/about-us/careers/adviser-aps6-rs-september-2015, taking into consideration the duties of the position as well as the capabilities.
Increase in iappANZ membership fees

As outlined on page 4, iappANZ has now introduced a membership fee increase and a new tiered fee structure as of 1 August 2015. The membership fees that apply from 1 August 2015 are set out below (note that fees are in Australian dollars):

<table>
<thead>
<tr>
<th>Membership Type</th>
<th>Fee</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Standard Membership</strong></td>
<td></td>
</tr>
<tr>
<td>Individual</td>
<td>$250 incl. GST</td>
</tr>
<tr>
<td>Corporate</td>
<td>$225 incl. GST per Member</td>
</tr>
<tr>
<td>3-4 Members (10% discount)</td>
<td>$675 incl. GST (3 Members)</td>
</tr>
<tr>
<td></td>
<td>$900 incl. GST (4 Members)</td>
</tr>
<tr>
<td>5+ Members (15% discount)</td>
<td>$212.50 incl. GST per Member</td>
</tr>
<tr>
<td></td>
<td>$1062.50 incl. GST (5 Members)</td>
</tr>
<tr>
<td><strong>Government/Not-for-Profit/Senior (60+)</strong></td>
<td></td>
</tr>
<tr>
<td>Membership</td>
<td></td>
</tr>
<tr>
<td>Individual</td>
<td>$225 incl. GST</td>
</tr>
<tr>
<td>Corporate</td>
<td>$202.50 incl. GST per Member</td>
</tr>
<tr>
<td>3 - 4 Members (10% discount)</td>
<td>$607.50 incl. GST (3 Members)</td>
</tr>
<tr>
<td></td>
<td>$810 incl. GST (4 Members)</td>
</tr>
<tr>
<td>5+ Members (15% discount)</td>
<td>$191.25 incl. GST per Member</td>
</tr>
<tr>
<td></td>
<td>$956.25 incl. GST (5 Members)</td>
</tr>
<tr>
<td><strong>Student (University Full-time)</strong></td>
<td>First year complimentary</td>
</tr>
<tr>
<td></td>
<td>$25 for second and remaining years if full-time university study</td>
</tr>
</tbody>
</table>
PRIVACY@WORK Summit

Connect and enhance your privacy knowledge

Hear from three international privacy thought leaders **Bojana Bellamy (UK)** – President, Centre for Information Policy Leadership, Hunton & Williams LLP, **Marie Shroff (NZ)** – former New Zealand Privacy Commissioner and *iappANZ Privacy Hall of Fame* inductee, **Hilary Wandall (USA)** – Assoc. Vice President, Compliance + Chief Privacy Officer, Merck.

Webcam, by kind permission of artist, Sherry Karver, Rebecca Hossack Gallery

Three keynotes, five panel discussions, 24 panelists exploring themes: *Managing Privacy – a stakeholder perspective, Metadata Conversation, New Technologies and Privacy Impacts, Privacy in Sport* and *The Politics of Privacy*.

**When:** Wednesday 18 November, 9.00am – 6.30pm, incl. networking time

**Where:** ZINC, Federation Square, Melbourne

**Earlybird:** Until 7 October

**Details:** [www.iappanz.org/events](http://www.iappanz.org/events)

Join us for a full day of insightful information and discussion regarding best practices, new trends and guidance on opportunities in the field of privacy.
## Privacy Events

<table>
<thead>
<tr>
<th>Time, Date &amp; Location</th>
<th>Information</th>
<th>Price</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>MELBOURNE</strong>&lt;br&gt;Monday 26 October 5.00pm – 7.00pm</td>
<td>Top tips to becoming a good privacy professional&lt;br&gt;Are you multitasking where privacy compliance is a part of your job? Are you interested in the privacy arena but don’t know enough about it? Do you want to know more about becoming a privacy specialist?&lt;br&gt;iappANZ invites you to a casual discussion with two privacy experts (David Templeton from ANZ and Ben Carr from Telstra) who can demystify the world of the privacy professional and offer top tips on how to become a good privacy officer.</td>
<td>Check iappANZ website for registration details (details coming soon at iappanz.org/Events)</td>
</tr>
<tr>
<td><strong>BRISBANE</strong>&lt;br&gt;Wednesday 28 October 12.30pm – 2.00pm (incl. a light lunch)</td>
<td>The Hacker, the Lawyer, the Client 2016 Privacy Breach Hypothetical&lt;br&gt;When client information is spilt, you risk losing the client. A privacy breach is a breach of trust. Loose the trust and you may well loose the client.&lt;br&gt;It may happen because someone forgot to use the shredder or a secure web service. It may happen in your reception when information is being collected. Whatever the reason, odds are that it will happen - the dreaded privacy breach.&lt;br&gt;Everyone is needs to know how it happens, how to stop it and what to do when it does.&lt;br&gt;This ‘Hypothetical’ session will provide real life scenarios and expert insights to give the audience a checklist of what to do and what to avoid.&lt;br&gt;We will take questions before the event – just don’t email them to us under your name!</td>
<td>Free for iappANZ members $99 for non-members Costs deductible from joining fee Check iappANZ website for registration details (details coming soon at iappanz.org/Events)</td>
</tr>
</tbody>
</table>
### WELLINGTON and AUCKLAND

**Thursday 5 November**

**In Wellington:**

12.00pm – 2.00pm  
Venue: Chapman Tripp  
L17, 10 Customhouse Quay  
Maritime Tower, Wellington  
(a light lunch will be served)

Also in Auckland (see details below)

3.00 – 5.00pm  
Venue: Simpson Grierson  
L28, Lumley Centre  
88 Shortland Street, Auckland  
(followed by refreshments and networking)

### Privacy & Security Terms for Cloud Computing Contracts

The use of cloud computing services is increasingly relied upon by businesses of all sizes. Personal information is increasingly finding its way into the hands of third party cloud providers and outside of the immediate reach of the business.

This interactive session, in partnership with Chapman Tripp in Wellington and Simpson Grierson in Auckland, will cover the obligations and risks to consider when reviewing or drafting contract terms for cloud computing services to protect the privacy of personal information that belongs to your business. It will also provide you with an opportunity to talk with legal and privacy experts used to managing the contractual requirements of cloud computing.

**Highlights:**

- Hear about key obligations and risks relating to privacy and security that your business should consider when procuring cloud services, and how these may be addressed in your cloud services agreements
- Be more aware of the possible pitfalls of cloud computing for privacy and the security of personal information and gain some tips on how you can avoid them
- Analyse sample clauses from a generic customer / cloud vendor contract
- Understand the types of cloud vendor contracts and clauses that may be negotiable and possible risk mitigation steps that can be taken when faced with non-negotiable terms.

### MELBOURNE

**Wednesday, 18 November 2015**

All day event 8am-6pm  
Venue: Zinc at Federation Square, MELBOURNE

### iappANZ annual Privacy Summit

See page 34 for details of keynote speakers

Full program to be published soon!

Contact Emma Heath for further information – emma.heath@iappanz.org

### REGISTER HERE.

**Earlybird (until 7 October 2015):**
- iappANZ member: $637.50 incl. GST;  
- Non-member: $857.50 incl. GST.  
Non-member registration fee includes annual iappANZ membership

**After 7 October 2015:**
- iappANZ Member: $687.50 incl. GST  
- Non-member: $907.50 incl. GST
IAPP Certification

Privacy is a growing concern across organizations in the ANZ region and, increasingly, privacy-related roles are being made available only to those who can demonstrate expertise. Similar to certifications achieved by accountants and auditors, privacy certification provides you with internationally recognized evidence of your knowledge, and it may be the edge you need to secure meaningful work in your field.

Our global body, the International Association of Privacy Professionals (iapp) says:

‘In the rapidly evolving field of privacy and data protection, certification demonstrates a comprehensive knowledge of privacy principles and practices and is a must for professionals entering and practicing in the field of privacy. Achieving an IAPP credential validates your expertise and distinguishes you from others in the field.’

What certifications are available? Are they relevant to my work here?

The iapp offers six specialised credentials, two of which are particularly relevant to iappANZ members, namely the Certified Information Privacy Professional/Information Technology (CIPP/IT) and the Certified Information Privacy Manager (CIPM).

To achieve either of these credentials, you must first successfully complete the Certification Foundation. The Certification Foundation covers basic privacy and data protection concepts from a global perspective, provides the basis for a multi-faceted approach to privacy and data protection and is a foundation for the distinct iapp privacy certifications.

What about testing?

Certification testing is available to iappANZ members locally (at iapp-approved computer-based testing centres). The iapp manages certification registrations and materials, and you can set an appointment to sit your exam online at a testing centre in Australia or New Zealand.

Our contact details

*Privacy Unbound* is the journal of the International Association of Privacy Professionals, Australia-New Zealand (iappANZ), PO Box 193, Surrey Hills, Victoria 3127, Australia ([http://www.iappanz.org/](http://www.iappanz.org/))

If you have content that you would like to submit for publication, please contact the Editors:

**Veronica Scott** (veronica.scott@minterellison.com)  
**Carolyn Lidgerwood** (carolyn.lidgerwood@riotinto.com)

*Please note that none of the content published in the Journal should be taken as legal or any other professional advice.*